Cryptanalysis of an Improved User Authentication Scheme with User Anonymity for Wireless Communications

l-iberty(l-iberty@foxmail.com)
Department of CS
UESTC, Chengdu, Sichuan, 611731

April 20, 2019

Abstract

A user identity anonymity is an important property for roaming services. In 2011, Kang et al. proposed an improved user authentication scheme that guarantees user anonymity in wireless communications.
key words: *cryptanalysis, authentication, anonymity, wireless communication, security*

1 Introduction

2 Review of Kang et al.'s Scheme

2.1 Initial Phase

When an MU registers with his/her HA, the MU's identity ID_{MU} is submitted to the HA. After receiving ID_{MU} from MU, HA generates PW_{MU}, r_1 and r_2 as follows.

$$PW_{MU} = h(N \parallel ID_{MU}) \tag{1}$$
$$r_1 = h(N \parallel ID_{HA}) \tag{2}$$
$$r_2 = h(N \parallel ID_{MU}) \oplus ID_{HA} \oplus ID_{MU} \tag{3}$$

where N is a secret value kept by HA. HA stores ID_{HA}, r_1, r_2 and $h(\cdot)$ in the smart card of MU and then sends it with PW_{MU} to MU through a secure channel.

2.2 First Phase

Figure 1 illustrates the first phase of Kang et al.'s scheme. A foreign agent FA authenticates MU by interacting with HA as follows.

1. $MU \rightarrow FA : \{n, (h(ID_{MU}) \parallel x_0 \parallel x), ID_{HA}, T_{MU}\}$
   If MU inputs ID_{MU} and PW_{MU} to MU's mobile device, then MU's mobile device chooses secret random

Table 1: Notations.

HA	Home Agent of mobile user
FA	Foreign Agent of the network
MU	Mobile User
PM_{MU}	A password of MU
N	A strong secret key of HA
ID_A	Identity of an entiry A
$E_{P_A}(X)$	Encryption of message using public key of A
$S_{S_A}(X)$	Signature on message using private key of A
$h(\cdot)$	A one-way hash function
$\parallel$	Concatenation
$\oplus$	Bitwise exclusive-or operation

values x_0 and x and computes n and L as follows.

$$n = h(T_{MU} \parallel r_1) \oplus r_2 \oplus PW_{MU} \tag{4}$$
$$L = h(T_{MU} \oplus PW_{MU}) \tag{5}$$

MU's mobile device sends MU's login message $\{n, (h(ID_{MU} \parallel x_0 \parallel x))_L, ID_{HA}, T_{MU}\}$ to FA, where T_{MU} is a current timestamp.

2. $FA \rightarrow HA : \{b, n, (h(ID_{MU}) \parallel x_0 \parallel x)_L, T_{MU}, S_{S_{FA}}, ((h(ID_{MU}) \parallel x_0 \parallel x_L, T_{MU}, Cert_{FA})), Cert_{FA}, T_{FA}\}$
FA checks the validity of T_{MU}. If it is valid, then FA chooses secret random number b. FA then sends b, the MU's login message containing $\{n, (h(ID_{MU} \parallel x_0 \parallel x))_L, ID_{HA}, T_{MU}\}$, a certificate $Cert_{FA}$, timestamp T_{FA}, and the corresponding signature on the login message by FA's private key S_{FA} to HA.

3. $HA \rightarrow FA : \{c, W, S_{S_{HA}}(h(b, c, W, Cert_{HA})), Cert_{FA}, T_{HA}\}$
HA checks the validity of certificate $Cert_{FA}$ and timestamp T_{FA}. If they are valid, then HA computes MU's real identity ID_{MU} as follows.

$$ID_{MU} = h(T_{MU} \parallel h(N \parallel ID_{HA})) \oplus n \oplus ID_{HA} \tag{6}$$

HA computes $L = h(T_{MU} \parallel h(N \parallel ID_{HA}))$ with his/her secret N and decrypts $(h(ID_{MU}) \parallel x_0 \parallel x)$. Then, HA verifies if MU is a legal use by checking $h(ID_{MU}) = h(ID_{MU})\prime$, where $h(ID_{MU})$ is computed with ID_{MU} on the login message and $h(ID_{MU})\prime$ of the decrypting result $\{h(ID_{MU})\prime \parallel x_0\prime \parallel x\prime\}$.

2.3 Second Phase

When MU visits FA at the i-th session, MU sends the following login message to FA.

1. $MU \rightarrow FA : TCert_{MU}, (x_i \parallel TCert_{MU} \parallel \text{Other Information})_{k_i}$
The new i-th session key k_i can be derived from the unexpired previous secret x_{i-1} and the fixed secret value x as

$$k_i = h(h(h(N \parallel ID_{MU})) \parallel x \parallel x_{i-1}) \tag{7}$$

where $i = 1, \ldots, n$.

2. Upon receiving a login message from MU, FA decrypts $(x_i \parallel TCert_{MU} \parallel \text{Other Information})_{k_i}$ with k_i and newly saves $(TCert_{MU}, h(PW_{MU}), x_i)$ for the next communication.

3 Anonymity Problem of Kang et al.'s Scheme

Kang et al.[7] improved Wu et al.'s scheme[3] and Wei et al.'s scheme[6] to provide anonymity. ... as follows.

1. Any legal user MU can directly obtain $h(N \parallel ID_{HA})$ from r_1 in his/her smart card because $r_1 = h(N \parallel ID_{HA})$ from the Eq.(2).

2. The legal user ... as follows.

$$\begin{aligned} n\prime &= h(T\prime_{MU} \parallel r_1) \oplus r_2\prime \oplus PW\prime_{MU} \\ &= h(T\prime_{MU} \parallel r_1) \oplus h(N \parallel ID\prime_{MU}) \oplus ID_{HA} \oplus ID\prime_{MU} \oplus PW\prime_{MU} \\ &= h(T\prime_{MU} \parallel r_1) \oplus ID_{HA} \oplus ID_{MU} \end{aligned} \tag{8}$$

3. With obtained $r_1 = h(N \parallel ID_{HA})$ and collected message $\{n\prime, ID_{HA}, T\prime_{MU}\}$, MU can get the real identity $ID\prime_{MU}$ of the other mobile user $MU\prime$ as HA does at step (3) in the first phase as follows.

$$\begin{aligned} ID\prime_{MU} &= n\prime \oplus ID_{HA} \oplus h(T\prime_{MU} \parallel r_1) \\ &= h(T\prime_{MU} \parallel r_1) \oplus ID_{HA} \oplus ID\prime_{MU} \oplus ID_{HA} \oplus h(T\prime_{MU} \parallel r_1) \\ &= ID\prime_{MU} \end{aligned} \tag{9}$$

As a result, legal mobile user MU's anonymity cannot be preserved in Kang et al.'s scheme.

4 Conclusions

This letter demonstrated that recently published wireless authentication scheme by Kang et al. still cannot provide anonymity. Thereforem Kang et al.'s scheme did not solved the problem of user anonymity that was pointed out Zeng et.al [4] and Lee et al.[5].

Acknowledgements

This research is supported by Basic Science Research Program through the National Research Foundation of ...

References

[1] J.Zhu and J.Ma, "A new authentication scheme with anonymity for wireless environment," IEEE Trans.Consum.Electron.,vol.50.no.1,pp.230-234,2004.

[2] C.C.Lee, M.S.Hwang, and I.E.Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environ- ments," IEEE Trans. Ind. Electron., vol.53, no.5, pp.1683C1687, 2006.

[3] C.C.Wu, W.B.Lee, and W.J.Tsaur, "A secure authentication scheme with anonymity for wireless communications," IEEE Commun. Lett., vol.12, no.10, pp.722C723, 2008.

[4] P.Zeng, Z.Cao, K.R.Choo, and S.Wang, "On the anonymity of some authentication schemes for wireless communications," IEEE Com- mun. Lett., vol.13, no.3, pp.170C171, 2009.

[5] J.Lee, J.H.Chang, and D.H.Lee, "Security flaw of authentication scheme with anonymity for wireless communications," IEEE Commun. Lett., vol.13, no.5, pp.292C293, 2009.

[6] Y.Wei, H.Qiu, and Y.Hu, "Security analysis of authentication scheme with anonymity for wireless environments," ICCT (International Conference on Communication Technology), 2006.

[7] M.Kang, H.Rhee, and J.Choi, "Improved user authentication scheme with user anonymity forwireless communications," IEICE Trans. Fundamentals, vol.E94-A, no.2, pp.860C864, Feb. 2011.